Numbers, Please

Fraud in Digital Advertising: A Multibillion-Dollar Black Hole

How Marketers Can Minimize Losses Caused by Bogus Web Traffic

GIAN M. FULGONI
comScore, Inc.
gfulgoni@comscore.com

INTRODUCTION

Fraud long has been known to be one of the most troublesome issues on the Internet, with digital advertising increasingly one of its prime victims (Edelman, 2014; Interactive Advertising Bureau, 2015; Springborn and Barford, 2013). The Association of National Advertisers (ANA) in late 2015 estimated that marketers will waste as much as $7 billion globally in 2016, buying online advertisements that people do not see.[1]

Fraudsters succeed by creating their own websites and using fake audiences to attract advertisers or by charging legitimate publishers to direct invalid traffic to their sites. The ANA findings showed that display and video advertisements bought using automated systems are a big part of the problem, and they have a significantly higher level of fraud compared with advertisements that were purchased directly through human sales forces. ANA chief Bob Liodice criticized the industry for being slow to take action and urged it to do more to fix the vexing problem.[1]

Another way in which fraud is affecting the digital advertising industry is by creating demand for ad blockers. This happens because the display advertisement ecosystem has permitted third-party software to run in some advertisement slots. That leeway, however, has allowed malicious code to be run in advertisements, resulting in users getting infected with viruses and malware. The use of ad blockers then becomes a simple and secure way for consumers to protect themselves, making it increasingly difficult for marketers to communicate directly with them.

Faced with these challenges, smart marketers need to respond in a variety of creative and sophisticated ways to ensure they can still reach their target segments in a cost-effective manner.

[1] *"The Bot Baseline: Fraud in Digital Advertising." Retrieved March 9, 2016, from Association of National Advertisers website: http://www.ana.net/content/show/id/botfraud-2016*

THE FAKE TRAFFIC SYNDROME

Much of today's advertisement fraud occurs because of so-called invalid, or nonhuman, traffic (IVT) that receives advertising impressions paid for by the advertiser, when in reality a human never actually sees the advertisement. It goes without saying that advertisements not seen by humans have no hope of affecting consumer behavior (Flosi, Fulgoni, and Vollman, 2013). Beyond not having an impact, this IVT also undermines the integrity of every other performance and effectiveness metric. If IVT isn't eliminated from measurement, then all key performance indicators are adversely infected.

IVT can be defined as traffic to a website that is generated—either intentionally or unintentionally—by invalid sources. Eliminating it requires identifying all of the variations of IVT and deploying measurement that continuously evolves as new types of invalid activity surface in the digital ecosystem. Types of IVT include

- traditional bots: systems designed to mimic human users and drive up advertising impressions;
- adware and browser "hijacks": software that makes html or "ad calls" without the user's knowledge. The malware running on the user's device (laptop, tablet, etc.) redirects the user experience to achieve the tamperer's goal—making money from fake traffic;
- ad injectors: programs that maliciously insert advertisements into websites where they don't belong;
- domain laundering: low-quality sites that impersonate a high-quality publisher to steal advertisement sales;
- data-center traffic: originating from data-center devices without human users.

DOI: 10.2501/JAR-2016-024

Advertisers, agencies, and publishers alike feel the pain of IVT while the fraudsters benefit.

For media buyers, the negatives include

- wasted advertisement spending and decreased return on investment (ROI);
- lack of transparency into the drivers of performance; and
- missed opportunity for advertisements to have an impact.

For media sellers, IVT causes

- lack of trust in the value of their inventory;
- damage to their relationships with buyers; and
- loss of revenue to "long-tail" (less-trafficked) sites on the open exchanges.[2]

The ANA study reported that bots are able to fool many of the more simplistic detection and prevention systems, especially list-based prevention technologies used in the programmatic open ad exchanges. Knowledgeable marketers such as P&G, Unilever, and Nationwide increasingly are demanding the use of more sophisticated detection systems to help eliminate all IVT-delivered advertising impressions.[3]

Fraud long has been known to be one of the most troublesome issues on the Internet, with digital advertising increasingly one of its prime victims.

Why IVT Matters for Digital Audience Measurement

The ANA study referenced earlier reported that participating advertisers in 2015 cited bot percentage ranges in their advertising campaigns of between 3 percent and 37 percent, compared with between 2 percent and 22 percent in 2014. It is important to note that the study found that the overall rate of fraud remained high—basically unchanged over the two-year period—reflecting the reality that fake web traffic continues to plague the digital advertising industry.[4]

Forthcoming research by comScore, reflecting the same period, supports the ANA's campaign-specific findings.[5] Furthermore, on average, about 7 percent of digital advertising audiences are subject to IVT, such as fraud or nonhuman traffic. Although this rate is lower for premium publishers (about 4 percent), IVT levels are much higher (at least 8 percent) on the open exchanges.

It's also clear that more expensive forms of digital advertising attract higher levels of fraud. Video advertising bought on premium publisher sites, for instance, contains 5 percent IVT on average, whereas the open ad exchanges have much higher average IVT levels of 14 percent. The 2015 ANA study found that media with higher cost per thousand impressions (CPMs) were more vulnerable to bots as these platforms provide a stronger economic incentive for botnet operators to commit fraud. Display media with CPMs exceeding $10 had 39 percent higher bot levels than lower CPM media. Video advertisements with CPMs above $15 had 173 percent higher bot levels than lower-priced media.

When advertising impressions that are correctly targeted to humans are not separated from nonhuman impressions, it's impossible to get a true sense of a campaign's reach, frequency, and gross rating points (GRPs; Fulgoni, 2015). Making matters worse, these erroneous metrics often are fed into effectiveness, ROI, and marketing mix-model calculations, where bad inputs equate to bad outputs.

Invalid traffic also can affect demographic audience counts by obfuscating browser data and masquerading as a specific demographic segment. In other instances, IVT inadvertently is included in the demographic models used by researchers. When this happens, IVT is infecting demographic reporting, which means that media analysts could be acting off audience data that is inaccurate and misleading. Put another way, if IVT is not deleted, the reported demographic composition of digital audiences will be inaccurate, causing marketers to draw the wrong conclusions or to make poor optimization decisions.

Smart marketers are beginning to realize that audience delivery metrics and IVT removal must come from a single sophisticated reporting tool to be accurate.

Why IVT Matters for Viewability Measurement

There are two ways in which purchased digital advertisements may never be in view to consumers:

- First, even though a human is using the computer, the advertisements might not load on the viewable portion of the

[2] *Long-tail sites have an overall reach smaller than around 1.5 percent of the Internet population.*

[3] *"Some of the UK's biggest advertisers are coming together to establish a common definition for ad fraud." (2015, August 14). Retrieved March 10, 2016, from* The Drum *website: http://www.thedrum.com/news/2015/08/14/some-uk-s-biggest-advertisers-are-coming-together-establish-common-definition-ad*

[4] *"Bogus Web Traffic Continues to Plague the Ad Business." (2016, January 19). Retrieved March 9, 2016, from* The Wall Street Journal *website: http://www.wsj.com/articles/bogus-web-traffic-continues-to-plague-the-ad-business-1453204801*

[5] *Source: comScore's proprietary validated Campaign Essentials (vCE) norms database.*

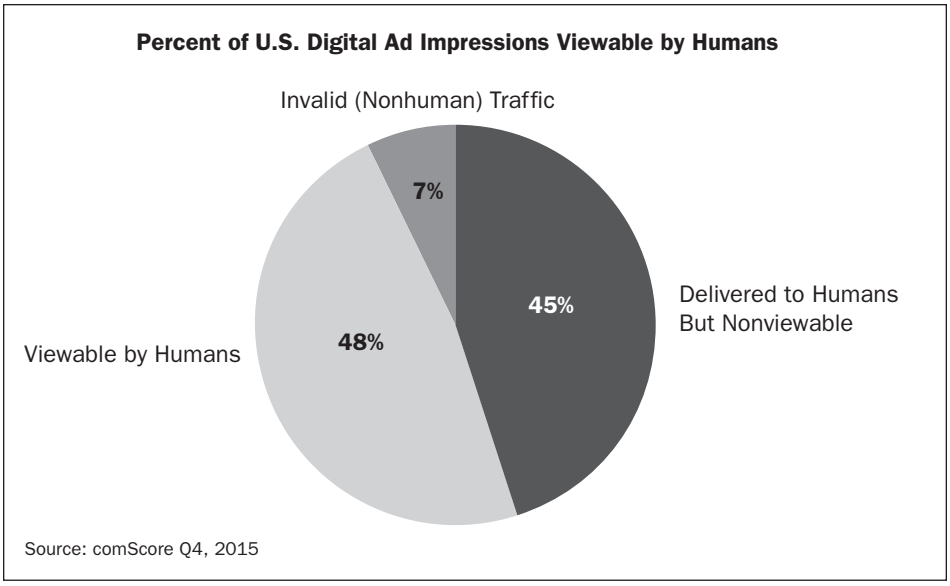

Figure 1 Viewable vs. Nonviewable Digital Advertisement Impressions

user's web page. An example of this is if the advertisement is loaded onto the page but below the computer screen and the consumer doesn't scroll far enough down the page to see the advertisement. These also are referred to as *out-of-view impressions*.

- The second way is if the advertisements are delivered to IVT.

In fact, less than half (48 percent) of desktop display and video advertisements are in view to the consumer. Fifty-two percent either are out of view to humans (45 percent) or delivered to IVT (7 percent; See Figure 1).

There is also wide variation in viewability by type of site, with premium sites having much higher in-view rates (55 percent) compared to lower levels (42 percent) on other sites. This difference can be traced, in part, to the lower levels of IVT on premium sites.

If a digital advertisement is served to IVT, should it be counted as viewable? No; but the IVT must be identified correctly. Suppliers of viewability measurement have reported large variation in levels of IVT for the same set of sites, according to a study led by the Media Ratings Council (MRC). The findings, supported by digital measurement practitioners and technical industry experts, led the MRC to draft a 2015 addendum to its earlier guidance for the detection and filtration of invalid digital traffic.[6] The addendum was intended to lead to improved measurement practices for detecting IVT. It identified two categories of IVT:

- general IVT and
- sophisticated IVT, which consists of more difficult-to-detect situations requiring advanced analytics, multipoint corroboration and coordination, and significant human intervention to analyze and identify IVT.

Leading marketers such as Unilever have insisted that all forms of fraudulent traffic are identified and—along with human out-of-view impressions—excluded from the counts of impressions delivered by a digital campaign.[7]

IVT and the Programmatic Ad Exchanges

As the buying of advertising impressions on open programmatic exchanges has increased, so have advertisers' concerns about fraud. In an ANA survey, 79 percent of advertisers said they had made programmatic buys in 2015—more than twice as many as in 2014 (35 percent).[8] Respondents to both the 2015 and 2014 surveys indicated that the leading benefits of programmatic buying were better targeting and real-time optimization.

Despite the significant growth, nearly 70 percent of the 2015 survey respondents still considered digital advertising fraud in programmatic buying to be a serious obstacle to the effective use of programmatic advertising. Roughly 31 percent said they have expanded their in-house capabilities to better manage programmatic ad buying. Additionally, marketers have taken other steps in response to transparency concerns:

- 62 percent requested detailed campaign guidelines and reporting from agency partners to ensure IVT fraud is being measured;
- 51 percent aggressively updated so-called "blacklists" of fraudulent sites;
- 45 percent targeted "whitelists" of low IVT sites;
- 42 percent purchased inventory through private marketplaces that media companies have created and where fraud levels are known to be lower.

[6] *"Invalid Traffic Detection and Filtration Guidelines Addendum." (2015, June 20). Retrieved March 9, 2016, from Media Ratings Council website: http://mediaratingcouncil.org/GI063015_IVT%20Addendum%20Draft%205.0%20(Public%20Comment).pdf*

[7] *"Almost a Quarter of Unilever's $8 Billion Ad Budget Is Now Spent on Digital." (2016, January 28). Retrieved March 9, 2016, from* Business Insider *website: http://www.businessinsider.com/unilever-digital-advertising-budget-up-to-24-2016-1*

[8] *"New Study Shows Huge Increase in Programmatic Ad Buying Among Top Marketers." (2016, March 3). Retrieved March 9, 2016, from ANA website: http://www.ana.net/content/show/id/38895*

How Fraud Triggers Use of Ad Blockers

One of the ways in which computers become infected with malware and subsequently become fraudulent bots is through the presence of infected advertisements on websites. Some of these advertisements pose as a trusted entity and present messages such as a system warning or a bogus security message. Scan advertisements of this type may make false claims that a system is out-of-date to encourage the installation of bogus software.

Google has been active in trying to protect Internet users by identifying a set of sites known to serve phishing or malware attacks. This list has been used by Chrome, Firefox, and Safari browsers for several years and recently was expanded to Android phones. In 2016, Google expanded its range of protection by targeting the actual deceptive embedded advertisements on any otherwise harmless site.[9]

Some consumers prefer to solve the fraud problem by using software to block all advertisements anywhere on the web. In the United States, about 10 percent of Internet desktop or laptop users have ad-blocking software installed on their computers.[10] The problem for advertisers becomes even more acute when one realizes that nearly 20 percent of young millennial men between the ages of 18 and 24 use ad blockers. This has sent marketers in search of alternative ways of interacting with this young and tech-savvy segment.

Native-branded content likely will be immune to ad blockers because the blocking software targets known ad servers (native content doesn't use ad servers). Therefore, it's to be expected that the use of branded content by marketers will increase. Other beneficiaries likely will be Facebook and Google or any other sites that serve their own advertisements and which the ad blockers would have trouble blocking.

Mitigating the Impact of Online Fraud

The challenges posed by online fraud notwithstanding, there are a number of options open to the digital advertising industry that can help minimize its impact. Most important is to ensure transparency by having buyers and sellers of advertising use campaign measurement tools that accurately identify all forms of nonviewable advertisements, including both general and sophisticated IVT.

Moreover, pricing negotiations between advertising sellers and buyers need to occur with a clear understanding of the degree to which advertisements are in view. Advertisers need to be extra vigilant when buying advertisements on open programmatic exchanges where fraud exists at high levels. The low price and targeting promise of the exchanges attracts advertisers, while fraudsters are lured by the volume of transactions. Insisting on viewable audience guarantees is one way for advertisers to minimize fraud.

Video advertising attracts advertisers because of its ability to lift sales. The high CPMs of video advertising also attract fraudsters, however, so advertisers need to be careful when buying on this platform, and it would be prudent to require some form of audience guarantee.

Meanwhile, advertising on premium publisher sites offers marketers the benefits of lower fraud, higher viewability and greater sales impact. Advertisers also need to ensure that inputs to market mix models only use validated viewable advertisements and not the gross tonnage delivered. Failure to do so will lead to erroneous conclusions that understate the impact of digital advertising.

Finally, because of the use of ad-blocking software by young millennials, marketers need to investigate ways to reach this segment that don't just rely on digital advertisements. The use of branded native content is one such approach. JAR

[9] *"Google will slap big red warning on legit sites hosting bad ads." (2016, February 4). Retrieved March 9, 2016, from ZDNet website: http://www.zdnet.com/article/google-will-slap-big-red-warning-on-legit-sites-hosting-bad-ads/*

[10] *"The State of Ad Blocking." Sourcepoint and comScore, September 2015. Retrieved March 9, 2016.*

ABOUT THE AUTHOR

Gian M. Fulgoni is cofounder and chairman emeritus of comScore, Inc. Previously he was president/ceo of Information Resources, Inc. During a 40-year career at the c-level of corporate management, he has overseen the development of many innovative technological methods of measuring consumer behavior and advertising effectiveness. Fulgoni is a regular contributor to the *Journal of Advertising Research*.

REFERENCES

Edelman, B. "Pitfalls and Fraud in Online Advertising Metrics: What Makes Advertisers Vulnerable to Cheaters, and How They Can Protect Themselves." *Journal of Advertising Research* 54, 2 (2014): 127–132.

Flosi, S., G. Fulgoni, and A. Vollman. "If an Advertisement Runs Online and No One Sees It, Is It Still an Ad?" *Journal of Advertising Research* 53, 2 (2013): 192–199.

Fulgoni, G. "Is the GRP Really Dead in a Cross-Platform Ecosystem? Why the Gross Rating Point Metric Should Thrive in Today's Fragmented Media World." *Journal of Advertising Research* 55, 4 (2015): 358–361.

Interactive Advertising Bureau. (2015, December 1). "What Is an Untrustworthy Supply Chain Costing the Digital Advertising Industry?" Retrieved March 9, 2015, from http://www.iab.com/insights/what-is-an-untrustworthy-supply-chain-costing-the-u-s-digital-advertising-industry/

Springborn, K., and P. Barford. "Impression Fraud in Online Advertising Via Pay-Per-View Networks." Paper presented at the 22nd USENIX Security Symposium, Washington, DC, August 2013. Retrieved March 10, 2016, from http://pages.cs.wisc.edu/~pb/usenix13_final.pdf